AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Apple Cellular Telephone (with a small photo of a unknown male within its casing) recovered pursuant to the arrest of Brianna CONTRERAS on 1/18/22

Case No. 22-1176MB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Arizona
(identify the person or describe the property to be searched and give its location):
Property described in Attachment A.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
Information/data described in Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before 2/24/2022
(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☑ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge James F. Metcalf .
(name)

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☑ for 30 days *(not to exceed 30)*.
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 2/10/2022 at 1:00 pm

Judge's signature

City and state: Yuma, Arizona

Hon. James F. Metcalf United States Magistrate Judge
Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is a One (1) Apple Cellular Telephone (with a small photo of a unknown male within its casing) recovered pursuant to the arrest of Brianna CONTRERAS on January 18, 2022 (hereinafter referred to as the "TARGET DEVICE," as further described in Attachment A). The TARGET DEVICE has been processed as evidence pursuant to the abovementioned arrest and HSI policy and procedure and is located at the HSI Evidentiary vault located at 7431 E. 30th St. Yuma, AZ 85365.

This warrant authorizes the forensic examination of the TARGET DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Property to be seized

Any records and information found within the digital contents of the TARGET DEVICE relating to any violations of 21 U.S.C. § 846 (Conspiracy to Possess with Intent to Distribute, a Controlled Substance), 21 U.S.C. § 841 (Possession with Intent to Distribute a Controlled Substance), and 21 U.S.C. § 952 (Importation of a Controlled Substance). Including but not limited to.

a. All information related to the sale, purchase, receipt, shipping, importation, transportation, transfer, possession, or use of drugs;
b. All information related to buyers or sources of drugs (including names, addresses, telephone numbers, locations, or any other identifying information);
c. All bank records, checks, credit card bills, account information, or other financial records;
d. All information regarding the receipt, transfer, possession, transportation, or use of drug proceeds;
e. Any information recording schedule or travel;
f. Evidence indicating the cellular telephone user's state of mind as it relates to the crime under investigation;
g. Contextual information necessary to understand the above evidence.
h. Any records and information found within the digital contents of the TARGET DEVICE showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" includes records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing

history; calendars; to-do lists; contact information; mapping and GPS information; data from "apps," including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the cellular telephone.

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Arizona

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Apple Cellular Telephone (with a small photo of a unknown male within its casing) recovered pursuant to the arrest of Brianna CONTRERAS on 1/18/22

Case No. 22-1176MJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Item described in Attachment A.

located in the _____ District of Arizona , there is now concealed *(identify the person or describe the property to be seized)*:

Information/data described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. SECTION 952	IMPORTATION OF A CONTROLLED SUBSTANCE
21 U.S.C. SECTION 841	POSSESSION WITH INTENT TO DISTRIBUTE A CONTROLLED SUBSTANCE

The application is based on these facts:

See Search Warrant Affidavit, Attachment A, and Attachment B from DEA Special Agent Henry Ochoa, incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Timothy Courchaine

Applicant's signature

Henry Ochoa. Special Agent DEA

Printed name and title

Sworn to telephonically.

Date: 2/10/2022

Judge's signature

City and state: Yuma, Arizona

Hon. James F. Metcalf, United States Magistrate Judge

Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is a One (1) Apple Cellular Telephone (with a small photo of a unknown male within its casing) recovered pursuant to the arrest of Brianna CONTRERAS on January 18, 2022 (hereinafter referred to as the "TARGET DEVICE," as further described in Attachment A). The TARGET DEVICE has been processed as evidence pursuant to the abovementioned arrest and HSI policy and procedure and is located at the HSI Evidentiary vault located at 7431 E. 30th St. Yuma, AZ 85365.

This warrant authorizes the forensic examination of the TARGET DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Property to be seized

Any records and information found within the digital contents of the TARGET DEVICE relating to any violations of 21 U.S.C. § 846 (Conspiracy to Possess with Intent to Distribute, a Controlled Substance), 21 U.S.C. § 841 (Possession with Intent to Distribute a Controlled Substance), and 21 U.S.C. § 952 (Importation of a Controlled Substance). Including but not limited to.

a. All information related to the sale, purchase, receipt, shipping, importation, transportation, transfer, possession, or use of drugs;
b. All information related to buyers or sources of drugs (including names, addresses, telephone numbers, locations, or any other identifying information);
c. All bank records, checks, credit card bills, account information, or other financial records;
d. All information regarding the receipt, transfer, possession, transportation, or use of drug proceeds;
e. Any information recording schedule or travel;
f. Evidence indicating the cellular telephone user's state of mind as it relates to the crime under investigation;
g. Contextual information necessary to understand the above evidence.
h. Any records and information found within the digital contents of the TARGET DEVICE showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" includes records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing

history; calendars; to-do lists; contact information; mapping and GPS information; data from "apps," including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the cellular telephone.

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANT

I, Henry Ochoa, being first duly sworn, hereby depose and state the following:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant to examine the cellular telephone further described in Attachment A (hereafter "TARGET DEVICE"), and to extract the electronically stored information set forth in Attachment B, which represent evidence and/or instrumentalities of the criminal violations further described below.
2. I am a Special Agent (hereinafter "SA") employed by the United States Department of Justice, Drug Enforcement Administration (hereinafter, "DEA"), and have been so employed with the DEA continuously since October 2015. Previously, your Affiant was employed with DEA from January 2011 until August 2012. I was also employed as a Task Force Agent with Homeland Security Investigations (hereafter "HSI TFA") from October, 2018 until February 1, 2022 to which my involvement in this matter was in said capacity.
3. As a DEA SA/HSI TFA, I have received specialized training in narcotics-trafficking and related crimes such as bulk cash smuggling. During my assignment with both DEA and HSI, I have participated in the execution of state and federal search warrants related to controlled substances. I am trained in methods of investigation to prosecute violations of federal controlled substance laws, including violations of Title 21, United States Code, Sections 841, 846, 952, 960, and 963.
4. I am an investigative law enforcement officer of the United States within the meaning of Title 21, United States Code, Section 878, and am empowered by law to conduct investigations and make arrests for offenses related to illegal narcotics-trafficking and related offenses.
5. In my capacity as a DEA SA, I am currently assigned to the Yuma Resident Office (hereinafter, "Yuma RO") of the DEA. In my capacity as a TFA, I was assigned to HSI in Yuma, AZ. I am responsible for investigating crimes that involve the unlawful importation, possession,

possession with intent to distribute, and distribution of illegal narcotics, the unlawful exportation of proceeds derived from the sale of illegal narcotics, and money laundering related offenses.

6. The statements contained in this Affidavit are based my observations, information derived from your Affiant's personal knowledge, training and experience, information obtained from the knowledge and observations of other sworn law enforcement officers, either directly or indirectly through their reports, surveillance conducted by law enforcement officers, and/or analysis of public records.

7. Because this Affidavit is being submitted for the limited purpose of establishing probable cause for the requested warrant, your Affiant has not set forth all the relevant facts known to law enforcement officers.

Identification of the Device to be Examined

8. The Warrant requests authorization to search One (1) Apple Cellular Telephone (with a small photo of an unknown male within its casing) recovered pursuant to the arrest of Brianna CONTRERAS on January 18, 2022 (hereinafter referred to as the "TARGET DEVICE," as further described in Attachment A). The evidence sought and expected to be stored within the TARGET DEVICE is described in Attachment B.

Probable Cause

9. On January 18, 2022, at approximately 8:07 A.M., Briana CONTRERAS attempted entry at the San Luis, Arizona Port of Entry (hereafter "POE"). CONTRERAS was the driver and sole occupant of a 2003 Hyundai Elantra. The vehicle was bearing Arizona license plate 81A35E and was registered to CONTRERAS. CONTRERAS claimed ownership of the vehicle to law enforcement.

10. While at the primary lane, the CONTRERAS stated to U.S. Customs and Border Protection Officers (hereafter CBPO's) that she was in Mexico "visiting her grandma" and that she was traveling to "work at Taco Bell in Yuma." Later, while retrieving biological data from the CONTRERAS she stated to Homeland Security Investigation agents that she was no longer employed.

11. CONTRERAS was referred to the X-ray/Z-Portal and after which, to secondary inspection for a further examination. In the secondary inspection area, the CBPO assigned to secondary was informed that there were anomalies discovered (via the X-ray/Z-Portal) in the quarter panels and the doors of the vehicle. During this period, a Canine Enforcement Officer (CEO) used an assigned K9, a Human and Narcotics Detection Dog, to conduct a search of the vehicle. The K9 alerted to said vehicle.

12. A subsequent search of the vehicle revealed approximately 80 packages located in numerous places within the vehicle. A random package was probed and found to contain a substance which field-tested positive for the characteristics of methamphetamine. The approximate weight of the packages discovered containing alleged methamphetamine was 33.60 kilograms. Also, the TARGET DEVICE, was recovered by CBPO's from the front passenger seat of the abovementioned vehicle.

13. Afterwards, agents attempted to conduct a post arrest, post Miranda, videotaped interview with CONTRERAS during which she stated that she would not talk to agents without an attorney present.

14. After conferencing the matter with AUSA Esther Winne, the matter was accepted for federal prosecution, and CONTRERAS was booked into the San Luis Regional Detention Center.

15. Based on the abovementioned circumstances, as well as your Affiant's training and experience, as well as the training and experience of other senior law enforcement officers participating in

this investigation, your Affiant has reason to believe that the TARGET DEVICE seized pursuant to the arrest of CONTRERAS was used in the furtherance of the importation and trafficking of illegal drugs to wit, 33.60 kilograms of Methamphetamine.

16. The TARGET DEVICE is currently in the possession of HSI Yuma, AZ. The TARGET DEVICE was discovered by CPB inside of the abovementioned vehicle at the abovementioned date, time, and location pursuant to the arrest. CBP subsequently transferred custody of the TARGET to HSI who processed it into evidence pursuant to HSI policy and procedure at the HSI Evidentiary vault located at 7431 E. 30th St. Yuma, AZ 85365.

17. In my training and experience, the TARGET DEVICE has been stored in a way that the contents are, to the extent material to this investigation, substantially the same state as when the TARGET DEVICE first came into the possession of the HSI.

18. Based on your Affiant's training and experience, as well as the training and experience of other senior law enforcement officers participating in this investigation, your Affiant knows that drug trafficking, bulk cash smuggling, and/or money laundering organizations and/or individuals (hereafter collectively referred to as "DTO") utilize cellular telephones (such as the TARGET DEVICE) to communicate when conducting their illegal activity, utilizing voice, text, and electronic mail functions of the cellular telephone to do so. These devices are utilized in furtherance of the crime by coordinating the transport and distribution of controlled substances, the collection and movement of currency, as well as communicating with members of the DTO about the specific operations of the DTO. Drug traffickers commonly use cellular telephones to communicate with other drug traffickers and customers about drug-related activities using telephone calls, text messages, email, chat rooms, social media, and other internet and application-based communication forums. Moreover, drug traffickers commonly

use other capabilities of cellular telephones to further their drug trafficking and money laundering activities. Therefore, evidence related to drug trafficking activity and money laundering activity is likely to be found on the TARGET DEVICE.

19. Additionally, your Affiant is aware that DTOs often use passenger vehicles and couriers to transport drugs from drug source locations in Mexico to distribution points within the United States. These locations are often unknown to the couriers and require the use of Global Position Satellite ("GPS") information, which may be accessed through the TARGET DEVICE. Furthermore, both the individual couriers, as well as the senior members of the DTO responsible for the transportation of drugs and bulk currency, utilize cellular telephones (such as the TARGET DEVICE) to coordinate the transfer and delivery of said items. Lastly, as a result, cellular telephones seized from individuals traveling in vehicles containing drugs intended for U.S. and originating in Mexico routinely contain information identifying not only the point of origin but also the intended destination of the drugs.

20. Based on my training and experience, including the facts learned in this investigation, I have reason to believe the following:

    a. DTO's must, by the very nature of their activity, communicate with their coconspirators. DTO's typically utilize various electronic devices including wireless telephones, computers, and tablets to facilitate these communications. The communications often occur via phone call, text message, email, social media, and/or messaging applications.

    b. DTO's often store names, contact information, and messages to and from their coconspirators in the memory of the electronic device and in memory cards for such

device. DTO's may also use these electronic devices to take photographs of drugs, money, firearms, and other assets, and store such photographs on their device.

c. Records of telephonic or text contacts between co-conspirators can corroborate statements by co-conspirators and can corroborate their testimony at trial or in grand jury proceedings. These records can also assist in identification of suppliers, distributors, and other participants in drug-trafficking offenses.

d. DTO's may use a GPS device to provide directions to locations that may be used to conduct drug transactions. In addition, a GPS device may record the user's location information, and that location information may be used to corroborate information received from other sources, or to help identify buyers, sources of supply, stash houses, and other locations and people of interest. In addition, cellular telephones are themselves often used as GPS devices.

e. DTO's often use online banking and money-transfer services to facilitate the purchase of and payment for illegal narcotics. DTO's may use wireless telephones, computers, and tablets to access these online banking and money-transfer services.

21. Searching the TARGET DEVICE for the evidence described above may require a range of data analysis techniques. In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, agents may be able to execute a "keyword" search that searches through the files stored in a computer for special words that are likely to appear only in the materials covered by a warrant. Similarly, agents may be able to locate the materials covered in the warrant by looking for directory or file names. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories; encode communications to

avoid using key words; attempt to delete files to evade detection; or take other steps designed to impede law enforcement searches for information. These steps may require agents to conduct more extensive searches, such as scanning areas of the device's memory not allocated to listed files or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant. Considering these difficulties, your Affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence.

22. Analyzing an electronic device for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Such devices utilize a vast array of different operating systems, software, and set-ups. The variety of hardware and software available requires even experts to specialize in some systems and applications. Thus, it is difficult to know prior to the search which expert possesses sufficient specialized skill to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since electronic evidence is extremely vulnerable to tampering or destruction (both from external sources and from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis. Furthermore, there are often no software tools designed for forensic searches of electronic devices.

23. Your affiant believes evidence relating to meet locations, hours of operation, stash-houses, telephone numbers being used, and/or co-conspirators presently unknown to investigators may be revealed by analyzing the TARGET DEVICE. In addition to items which may constitute evidence and/or instrumentalities of the crimes set forth in this Affidavit, your Affiant also

requests permission to seize any articles tending to establish the identity of persons who have dominion and control over the TARGET DEVICE.

24. Therefore, your affiant respectfully requests a search warrant be issued authorizing the search of the TARGET DEVICE seized incident to the arrest of CONTRERAS.

Digital Evidence stored within a cellular telephone

25. As described in Attachment B, this application seeks permission to search for records and information that might be found in the contents of the TARGET DEVICE. Thus, the warrant applied for would authorize the copying of electronically stored information under Rule 41(e)(2)(B).

26. *Probable cause.* Your Affiant submits that there is probable cause to believe records and information relevant to the criminal violations set forth in this Affidavit will be stored on the TARGET DEVICE for at least the following reasons:

    i. Your Affiant knows that when an individual uses a cellular telephone, the cellular telephone may serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The cellular telephone is an instrumentality of the crime because it is used as a means of committing the criminal offense. The cellular telephone is also likely to be a storage medium for evidence of crime. From my training and experience, your Affiant believes that a cellular telephone used to commit a crime of this type may contain data that is evidence of how the cellular telephone was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

    ii. Based on my knowledge, training, and experience, your Affiant knows that cellular telephones contain electronically stored data, including, but not limited to, records related to communications made to or from the cellular telephone, such as the associated telephone numbers or account identifiers, the dates and

times of the communications, and the content of stored text messages, e-mails, and other communications; names and telephone numbers stored in electronic "address books;" photographs, videos, and audio files; stored dates, appointments, and other information on personal calendars; notes, documents, or text files; information that has been accessed and downloaded from the Internet; and global positioning system ("GPS") information.

iii. Based on my knowledge, training, and experience, your Affiant knows that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a cellular telephone, deleted, or viewed via the Internet. Electronic files downloaded to a cellular telephone can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a cellular telephone, the data contained in the file does not actually disappear; rather, that data remains on the cellular telephone until it is overwritten by new data.

iv. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the cellular telephone that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a cellular telephone's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the cellular telephone was used, the purpose of the use, who used it, and when. There is probable cause that this forensic electronic evidence will be found in the contents of the TARGET DEVICE because:

i. Data in a cellular telephone can provide evidence of a file that was once in the contents of the cellular telephone but has since been deleted or edited,

or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

ii. As explained herein, information stored within a cellular telephone may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within electronic storage medium (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the cellular telephone. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the cellular telephone was remotely accessed, thus inculpating, or exculpating the owner. Further, activity on a cellular telephone can indicate how and when the cellular telephone was accessed or used. For example, as described herein, cellular telephones can contain information that log: session times and durations, activity associated with user accounts, electronic storage media that connected with the cellular telephone, and the IP addresses through which the cellular telephone accessed networks and the internet. Such information allows investigators to understand the chronological context of cellular telephone access, use, and events relating to the crime under investigation. Additionally, some information stored within a cellular telephone may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a cellular telephone may both show a particular location and have geolocation

information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The geographic and timeline information described herein may either inculpate or exculpate the user of the cellular telephone. Last, information stored within a cellular telephone may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within a computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence to conceal it from law enforcement).

iii. A person with appropriate familiarity with how a cellular telephone works can, after examining this forensic evidence in its proper context, draw conclusions about how the cellular telephone was used, the purpose of its use, who used it, and when.

iv. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a cellular telephone that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, cellular telephone evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on one cellular telephone is evidence may depend on other information stored on that or other storage media and the application of knowledge about how electronic storage media behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

v. Further, in finding evidence of how a cellular telephone was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For

example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your Affiant is applying for would permit imaging or otherwise copying the contents of the TARGET DEVICE, including the use of computer-assisted scans.

Conclusion

29. Your Affiant submits that, based upon the totality of the facts and circumstances described above, probable cause exists to search the TARGET DEVICE, described in Attachment A, for evidence (as listed in Attachment B) of violations of 21 U.S.C. § 846 (Conspiracy to Possess with Intent to Distribute, a Controlled Substance), 21 U.S.C. § 841 (Possession with Intent to Distribute a Controlled Substance), and 21 U.S.C. § 952 (Importation of a Controlled Substance).

30. In consideration of the foregoing, I respectfully request the Court issue the requested search warrant for the TARGET DEVICE and specifically grant authority to any member of a law enforcement agency authority to execute. Your affiant (as well as inter-agency law enforcement colleagues and partners) intends to examine manually, forensically, and/or electronically.

31. Because the requested search warrant seeks only permission to examine a device already in law enforcement's possession, the execution of the warrant does not involve physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the Warrant at any time of the day or night.

Henry Ochoa

Special Agent Henry Ochoa
Drug Enforcement Administration

Sworn to and subscribed before me telephonically on this 10th day of February, 2022.

HONORABLE JAMES F. METCALF
UNITED STATES MAGISTRATE JUDGE